بسم الله الرحمن الرحيم



هذا الموضوع أهديه ...
إلى جنــود وأنصــار ...
دولة العراق الإسلامية
:: مُحبكم في الله أبو طارق ::



##اعــرف عــدوك ##

|| التحقيـقُ الجنائــي الرَقَمــي ||

{{ خُلاصة المُحتوى العربي على الإنترنت حول التحقيق الجنائي الرَقمي }}

بعد قراءتك لهذه المقالة ستكون بإذن الله مُلماً بالكثير حول عمل المُحقق الجنائي الرَقمي من ناحية:
(ما يفعله عند سقوط الجهاز بين يديه ، عمله في المختبر ، لمحات حول بعض الأدوات والبرامج التي يستخدمها)

علماً أن أغلب المعلومات حول الأدوات والبرامج التي يستخدمها المُحقق لن تجدها على أي موقع عربي آخر



:: تهنئة ::

أهنئ أمة الإسلام عامة ، و وزراء ، وأمراء ، وجنود ، وأنصار دولة العراق الإسلامية خاصة ، على نيل أمير المؤمنين الشيخ أبو عمر البغدادي ، و وزير الحرب الشيخ أبو حمزة المهاجر الشهادة في سبيل الله ، نحسبهما كذلك ولا نزكي على الله أحد ، وأسأل الله أن يجمع أمير

المؤمنين ، و وزير الحرب بالأحبه محمد ـ صلى الله عليه وسلم ـ وصحبه ، وأن يربط على قلوب المُحبين ، وأن يوفّق جنود دولة العراق الإسلامية للمُضي قُدماً في إقامة دولة الإسلام ، التي تحكم بشريعة الرحمن ، لتكون لبنة في إقامة الخلافة الإسلامية ، وأن يُبدل دولة العراق الإسلامية خيراً منهما ، إنه هو البر الرحمن الرحيم



::المحتويات ::

{ 1 } -------------------- #مدخل إلى عالم الحشرات الإلكترونية.
{ 2 } -------------------- #دورة الدليل الرقمي في جرائم الإرهاب الإلكتروني 31-12-2009 .
{ 3 } -------------------- #الإجراءات الأوليّة للمُحقق الجنائي الرَقمي.
{ 4 } -------------------- #خطوات عمل المُحقق الجنائي الرَقمي في المُختبر .
{ 5 } -------------------- #لمحة حول بعض برامج وأدوات المُحقق الجنائي الرَقمي.
{ 6 } -------------------- #مواقع تُقدم أدوات ودراسات حول التحقيق الجنائي الرَقمي.
{ 7 } -------------------- #حاجة الجهاد الإعلامي والميداني إلى خبراء في " أمن المعلومات".
{ 8 } -------------------- #المُختبر التقني "الجهادي" لأمن المعلومات.
{ 9 } -------------------- #أسود "أمن المعلومات" المجاهدين أين هم؟. !!
{10} -------------------- #وسائل مُقترحة لِحماية "الأرشيف الجهادي" للمُجاهد الإعلامي .

||||||||مدخل إلى عالم الحشرات الإلكترونية ||||||||

نُعاني نحن الأعضاء في "رابطة عُشّاق المجاهدين " والمُرابطين خاصّة على ثغور الإعلام الجهادي ، من إزعاج بعض الحَشرات الضّارة ، التي تجتهد في البحث عن كل من يُفكر في معارَضة الذبابة الأمريكية لتلتهمه ، فهي تهاجم كل من

يُحارب الرَذيلة والهزيمة ، مُستخدمة أسلحتها المتطورة ، فتارة تستخدم سلاح تحديد IP الفريسة ، لتختطفه من وسط بيت أمه ، وتارة ترتدي وشاح الفضيلة ، وتدعوا للسكينة ، والبُعد عن كل عزيمة.!!

والحشرات الضّارة مُتنوعة الأشكال، والأحجام، والجنسيات أيضاً !!، فهناك الخنافس الأوربية ، والديدان اليهودية ، واليَرَقات الأفريقية ، ولكن أخطرها على الإطلاق ، وأكثرها إخلاصاً للذبابة الأمريكية ، هي البعُوضة العربية السمينة ،التي تشتهي دمائنا ، فهي تشرب منها في يقظتها ، وتحلم بها في منامها، وتنتشر بكثرة في مُستنقعات الشرق الأوسط الإلكترونية .

ففي حياتنا الواقعية نُعاني من رجل أمن الدولة المغوار ، بتقنياته الفذّة المُستخدمة في الإيقاع بالمجاهد ، وأهله ، وأقاربه ، وجيرانه ، بل وأحياناً بألد أعدائه!!

فترى هذا المخلوق الغريب في كل مكان ، فهو في مَحل عملك ، يلعن ولي الأمر كُلما دخلت عليه ليَستدرجك، وهو بجانبك في المسجد يلعن من يلعن ولي الأمر ليتأكد من وَلائِك ، وهو خلفك في طابور المخبز يلعن الخباز ويلعنك ويلعن نفسه . !!

فأمنيته في الحياة أن يُدخل كل الكائنات الحيّة إلى سجن ولي الأمر، الذي يتسع للجميع .

ففي الصباح يكتب تقرير عن مديره في العمل ، وقبل الظهر يُدلي بشهادة زور على جاره المحافظ على الصلاة في المسجد ، وبعد الظهر يُشارك في أحد المنتديات الأثرية مبيناً سِعة حِكمة ولي الأمر التي باتت بحجم ال1000كيلوبايت ، وبعد العصر يمكث في المسجد ليُراقب كل التحركات المشبوهة في حلقة تحفيظ الأطفال !!وبعد المغرب يقف خلفك في طابور المخبز مكرراً طقوس اللعن اليومي ، وبعد العشاء يبدأ في صياغة التقرير الذي سيُدخلك به السجن من أوسع أبوابه.!!

كل هذا جعلنا مضطرين للهجرة إلى الحياة الافتراضية على شبكة الإنترنت.

ففي شبكة الإنترنت نحمل هوية أخرى، غير الهوية المُرقمّة التي صُرفت لنا في بُطون أمهاتنا ليسهُل اصطيادنا لاحقاً، إن خرجنا عن الطريق الذي رسمه لنا الدعاة على أبواب جهنم .

وعلى الإنترنت نستطيع أن نُعبّر عن مشاعرنا الوردية تجاه ولي الأمر، وجنود ولي الأمر، وعلماء ولي الأمر، تلك المشاعر الصافية والنقية، كقلب أبو الخير -رحمه الله!! (1)-، وتلك الأحاسيس الدافئة التي لا تُترجمها الكلمات ، ولا نستطيع إيصالها إلا بهدية كهدية المعبدي -رحمه الله.!! (2)-

وعلى الإنترنت نلتقي بأحبة لنا نتمنى لو نستطيع استنساخهم، وحفظهم في ملفات مضغوطة، بكلمات سريّة مُعقدة، ليكونوا بعيدين عن أعين المخلوقات الغريبة.

هذه الحياة الواقعية التي جعلت "رابطة عُشاق المجاهدين" تهاجر إلى الإنترنت ، جعلت منهم أيضاً خُبراء في الأمور التقنية ، فترى الواحد منهم لم يرى جهاز الحاسب الآلي ، إلا بالأمس ، يُشارك اليوم في المُنتدى الجهادي ، ويشرح غداً فن التخفي والتشفير المُتطور، مع لمحة تاريخية مُوجَزة عن تطور هذا الفن للأعضاء الجُدد.!!

فأصبح أسود الإعلام الجهادي بفضل الله ، أصحاب خبرة "خُرافية" في فنون التخفي والتشفير ، يُنافسون بها أجهزة

الاستخبارات العالمية العريقة ، فأنا أحدثكم الآن من ألمانيا ، وبعد دقيقتين من وسط أمريكا ،وبعد 3دقائق من أديس أبابا !!، فنحن نسبح في أنفاق التشفير، ونعوم في أعماق التقنية الغربية ، التي جعلها الله لنا غنيمة باردة ...

نُرهبُهم بها ، ونُحرّضُ أهلنا عليهم بها ، ونُخطط ونتواصل فيما بيننا بها .

ولكن...هل هذا يكفي للوقاية من البعُوض العربي السمين المُتعطش لدمائنا ؟.!!

في الحقيقة إن العلاقة العاطفية بين المجاهدين وأجهزة أمن الدولة ، أكبر من كل ذلك ، فالحكومات العربية تسعى جاهدة لحمايتنا من الانقراض وذلك بتكديسنا في مخازنها الصحراوية "المُكَيّفة "بالطبع ، وأما الشخصيات المُهمة من المجاهدين وأنصارهم ، فلهم مخازن خاصة في باطن الأرض لحمايتهم من الأوكسجين الضار!!

إذاً...فالواجب علينا مراقبة هذه الحشرات ، وخاصة البعُوضة العربية، ومعرفة تحركاتها ، وأدواتها التي تُسهّل لها تحديد أماكننا ، وطرق تفكيرها ، لنتعرف على نقاط ضعفها ، ونأخذ حَذرَنا منها ، ونُجهّز المُبيد الحَشري المناسب إن توفَّر ...

وإلا ..فنعلُ أحَدِنا يكفي لألف ألف بعُوضة.

||||||||دورة الـدليـل الـرَقمي في جـرائم الإرهـاب الإلكتـروني 31-12-2009 ||||||||

يُعرف عن الحكومات العربية تخلفها الشديد في جميع المجالات ، العلمية ، والاقتصادية ، والعسكرية ، والطبية ، وغيرها من المجالات ، وعندما سَعت هذه الحكومات أخيراً لإدخال خدمات الاتصالات الحديثة ، وتقنيات الـ GPS ، وغيرها من التقنيات المُتطورة ، كان هدفها بالدرجة الأولى بوليسي ، لاستخدامها في مراقبة الشعب والتجسس عليه ، ولا تزال الحكومات العربية المُتخلفة ، تسعى جاهدة لجلب كل التقنيات الحديثة ، التي تجعل المواطن المغلوب على أمره ، تحت أعينها ، لخدمته بالطبع ، وخدمة أهله ، وأقاربه ، وجميع معارفه ، "خاصة "الذين ابتلاهم الله بإصابة فَلذة كبدهم بفيروس "العِزّة " ، والذي سبّب بدوره سُقوط الغشاوة من أمام عيني ابنهم ، مما جعل عورة الآنسة "حكومة " مكشوفة أمامه ، فصار تبعاً لذلك يصيح في أهله وقومه ، مبيناً لهم ردّة الحكومة "المُحجبة" المتزوجة سراً من الفحل الأمريكي.!!

و أما صور جلب التقنية الحديثة ، وعقد الدورات حولها ، فهي متعددة في دول العالم الثالث ، وكان من آخرها ما حصل في دولة قاعدة العُديد !! (3)، وهذا الاسم أشهر من أسم الدولة المُستضيفة، أعني جزيرة قطر، حيث ورد في موقع وزارة داخلية الدولة المذكورة التالي:

"أختتم في صباح يوم الخميس 31-12-2009 في مركز مكافحة الجرائم الإلكترونية التابع لإدارة البحث الجنـائي في قطر دورة ((الـدليـل الـرقمي في جرائم الإرهـاب الإلكتـروني)) ، التي نظمتها - جامعة نايف العربية للعلـوم الأمنيـة - بالتعاون مع وزارة داخلية قطر "و شارك فيـها **7** دول عربية وهي:

"قطر، والسعودية، والكويت، وسوريا، والسودان، ولبنان، وليبيا"

وقد علقّت بعُوضة من جامعة نايف الأمنية على الدورة فقالت:

"أن هذه الدورة تأتي في إطار مكافحة الإرهاب الإلكتروني والإرهاب بشكل عام ، ومن بين البرامج التي يجب أن يكون ملماً بها رجل مكافحة الإرهاب هي الجرائم الإلكترونية ، وكما يمكن من خلال الحاسوب وباستخدام الشبكة العنكبوتية أن تنتقل الشفرات والخطط الإجرامية بين أفراد العصابات في أنحاء العالم ، وهذه الأمور كلها أصبح الآن بالإمكان مراقبتها إلكترونيا ، حتى الوصول إلى الأجهزة المُستخدمة في تلك العمليات الإرهابية واستخلاص الدليل منها وتقديمه للمحكمة شأنه في ذلك شأن الأدلة التي تقدم في الجرائم التقليدية ، وهناك العديد من الدول التي اعتمدت التقارير والدلائل المستخلصة إليكترونيا كأدلة إدانة في قضايا الإرهاب الإلكتروني.(4)"

إذاً .. صار بالإمكان الآن ، تحديد أماكننا ، ومعرفة سلاح الجريمة ، الذي قد يكون حاسب محمول من نوع كلاشنكوف !!، أو لوحة مفاتيح مُفخخة !!، فهل بعد هذا سنتهاون من الناحية الأمنية، حتى نجد أنفسنا كوجبة شهية، بين يدي بعُوضة عربية جائعة و مُتخلفة ؟.!!

أما الرائع في "دورتهم الأمنية " أنها أختتمت في يوم الخميس 31-12-2009 ، بعد أن تعلموا أحدث التقنيات للوصول إلى أسود الإعلام الجهادي كما يزعُمون ؟.!!

وفي نفس هذا اليوم وصل بحمد الله أحد أسود الإعلام الجهادي إلى قاعدة شابمان الأمريكية في خوست، فكبر بين كبار قادة الـ CIA ثم فجر ، فهل عَرفتموه(5)؟!! وهل يعتبر البعُوض مما جرى لسيدتهم الذبابة؟.!!



||||||||الإجراءات الأوليّة للمحقق الجنائي الرَقمي ||||||||

الكثير من أسود الإعلام الجهادي ، لا يعلم عن طبيعة عمل المُحقق الجنائي الرَقمي ، ولا يعلم أيضاً عن الذي يجري لحاسبه الشخصي ، إذا سقط في أيدي الأجهزة الأمنية، ويمكننا حصر الإجراءات الأولية التي يقوم بها المحقق الجنائي الرَقمي أثناء وقوع الجهاز بين يديه كالتالي:

{ 1 }يعمل على تأمين المنطقة التي يوجد فيها جهاز الحاسب.

{ 2 }يحرص على عدم تواجد أي شخص بالقرب من جهاز الحاسب، أو مصدر إمداده بالطاقة.

{ 3 }يَحذر من لمس أي شيء في الموقع، ماعدا الجهاز المُكلف به.

{ 4 }يقوم بلصق ملاحظات على جميع الأسلاك الموصولة بالحاسب مثل)سلك الشاشة، سلك لوحة المفاتيح (مبيناً عمل كل واحد منها.

{ 5 }يقوم بتصوير جهاز الحاسب من كل جهة ، ويلتقط صور أخرى للمكان الموضوع فيه الجهاز.

{ 6 }يبحث حول جهاز الحاسب الآلي عن أي قصاصات كُتب عليها كلمة سرية، أو بريد إلكتروني، أو ما شابه.

{ 7 }لن يُصغي المُحقق إلى نصيحة الأخ المُستخدم لجهاز الحاسب الآلي ، في حالة وقوعه في الأسر.

{ 8 }سيتأكد من حالة جهاز الحاسب الآلي، لأنه إن كان مغلق فلن يقوم المحقق بتشغيله أبداً، حتى لا يُحدّث سِجلات النظام بآخر تاريخ تشغيل، مما سَيُفسد عليه القضية "الإرهابية"، وبالتالي ستفسد عليه الترقية "الوظيفية!!"بل سيرسله إلى المختبر لمعالجته هناك ، وأما إن كان الحاسب في حالة سُبات ، فسيقوم المحقق بفصل التيار الكهربائي عنه و نقله إلى المُختبر ، وأما إن كان جهاز الحاسب يعمل بشكل طبيعي فسيقوم المحقق باستخدام برنامج مثل (COFEE) , لاستخراج كافة السجلات الخاصة بالنظام عن طريق الـ USB، وأخذ صورة للذاكرة المؤقتة، وتحليلها لاحقاً في المختبر.

{ 9 }سيقوم المحقق بوضع جميع ما يجمعه من (أقراص ليزرية ، أصابع ذاكرة الـ USB ، و الأقراص الصلبة الخارجية. وغيرها) ، في أكياس الأدلة ، المُضادة للشُحنات الساكنة ، لتجنب إتلافها من قبل المصادر المغناطيسية.

{10}سيقوم بنقل جهاز الحاسب المشتبه به ، إلى المُختبر لتشريحه(6).!!

||||||||خطوات عمل المحقق الجنائي الرَقمي في المُختبر ||||||||

في المختبر سيقوم المحقق بالكثير من الأعمال المُمتعة !!، من تحليل للبيانات المُستخرجة من الجهاز ، إلى مخاطبة مزودي خدمة الإنترنت ، وغيرهم من المتعاونين عن طيب خاطر، في الحرب الأمريكية "المُقدسة"على الإرهاب ، ليزوّدوه بسجلات مؤرخة عن مغامرات "الأخ "على الإنترنت ، وسجلات أخرى عن محادثاته العاطفية حول الجهاد والمجاهدين ، ومجلدات أخرى تحوي مشاركاته في المُنتديات الجهادية ، وغير ذلك من الأمور التي تساعد المحقق ، في تعليق الأخ "الأسير "على أحد أعواد المشانق الشاغرة ، في أقرب فرصة مُمكنة !!، أو في إقامة طقوس تكسير عظام الحاسب "المسكين!!"، في حالة نجاة الأخ من الأسر.
إذاً يجب علينا أولاً معرفة مما يتكون المختبر الجنائي الرَقمي ؟

يتكون المختبر الجنائي الرقمي من 4ركائز أساسية وهي:

{ 1 }أشخاص على قدر من المهنية العالية لديهم الخبرة الكافية والخلفية الواضحة بمتطلبات التحقيق.

{ 2 }مختبر مجهز بأدوات ومعدات لخلق بيئة عازلة لشحنات الكهرباء الساكنة، حيث تمنع انتقالها من الإنسان إلى الجهاز الإلكتروني الحاوي للأدلة، حتى لا تتعرض للتلف.

{ 3 }أدوات وتقنيات تحليل مناسبة، مع توفر أجهزة (Write Blocker) وهي أجهزة الهدف منها حماية جهاز المشتبه به، من أي عمليات كتابة عليه.

{ 4 }سياسات وإجراءات لعمليات حفظ الأدلة ، وتحليلها(7).

وأما عمل المُحقق الجنائى فى هذه المختبرات بعد نقل الجهاز إليها، فيمكننا حصره فى التالى:

{ 1 } إنشاء نسخة من الأدلة التي سوف يعمل عليها المحقق، لتجنيب أي ضرر يُمكن أن يحصل للدليل الأصلي من عملية التحليل في المختبر.

{ 2 } التأكد بأن النسخة التي أخذت عن القرص الصلب نظيفة (بدون فيروسات، أو ملفات تجسس).

{ 3 } استخدام جهاز مانع الكتابة (Write Blocker) لمنع كتابة أية بيانات على القرص الصلب الأصلي.

{ 4 } التأكد من مطابقة النسخة التي أخذت من القرص الأصلي ، عن طريق استخدام أكواد التشفير مثل (MD5 - SHA1) أو غيرها.

{ 5 } أخيراً يبدأ المحقق في فحص وتحليل القرص المُستنسخ من القرص الأصلي، واسترجاع الملفات المحذوفة منه، وغير ذلك من العمليات التي قد تساعد في إدانتك(8).!!

||||||||لمحة حول بعض برامج وأدوات المحقق الجنائي الرَقمي ||||||||

##غالبية المعلومات هنا لن تجدها على أي موقع عربي آخر ##

في البداية يجب أن تعلم أخي الغالي ، أن أجهزة أمن الحُكومات العميلة ، لا تقوم بأمور مُستحيلة ، و لا تمتلك عصا سحرية تصنع لها المُعجزات ، ولكن لديها أدوات وبرامج أغلبها متوفرة للجميع ، نعم قد يكون هناك بعض البرامج، والأدوات الحصرية للأجهزة الأمنية ، ولكن يوجد في مُقابلها أدوات ، وبرامج مجانية ، بل ومفتوحة المصدر أيضاً ، تقوم بنفس عمل الأدوات الحصرية ، والكثير من المُحققين الرَقميين الآن يعتمدوا على هذه البرامج والأدوات المجانية "مفتوحة المصدر" في قضاياهم الأمنية ، وذلك لأسباب كثيرة ، من بينها سهولة تطويرها من قبل المحقق نفسه ، وهذا يظهر جلياً في كتاباتهم على المواقع المُهتمة بالتحقيق الجنائي ، و على مُدوناتهم الشخصية أيضاً ، ولكن الذي يُميز الأجهزة الأمنية ، عن غيرها، هي التسهيلات التي تُقدم لها ، من شركات الاستضافة ومقدمي خدمة البريد الإلكتروني ، ومزودي خدمة الإنترنت ، وغيرهم ، وذلك بتنفيذهم لطلبات الأجهزة الأمنية ، وإمدادهم لها بكل المعلومات التي تريد ، حول أي حساب على مواقعها ، أو أي مُستفيد من خدماتها ، وأما عن الأدوات والبرامج المُستخدمة في التحقيق الجنائي الرَقمي ، فيمكنك أخذ فكرة عامة حولها في الأمثلة التالية لبعض هذه البرامج، والأدوات:

-1-

COFEE

Computer Online Forensic Evidence Extractor

طُور هذا البرنامج عام 2006 من قبل كل من Ricci Ieong و Anthony Fung، وكلاهما عضو في منظمة المحققين المُحترفين في جنوب آسيا (HTCIA)، ويحتوي برنامج COFEE على أكثر من 150 أداة ، وهي مُخصصة لأنظمة Windows، وهي من تطوير شركتي NW3C و Microsoft , وتسهّل هذه الأداة عمل المحققين في قضاياهم الرَقمية ، حيث تعمل هذه الأداة على جمع المعلومات من أجهزة المشتبه بهم مثل (البرامج التي تعمل في النظام ،

المواقع التي تم تصفحها ، كلمات المرور ، وغيرها الكثير) ومن ثم تخزينها في أصبع ذاكرة الـ USB،دون القيام بأي تعديلات على النظام ، ودون الحاجة لنقل الجهاز أو القرص الصلب إلى المُختبر ، وتقوم هذه الأداة بعرض المعلومات المسحوبة من جهاز المشتبه به ، على شكل مُستندات نصية ، أو على شكل واجهة رسومية حسب اختيار المحقق ، وهذه الأداة ليست للبيع ، ولكن توزع على الأجهزة الأمنية في العالم ، وقد تسربت نُسخة منها على الإنترنت ، وحصلت ضجة في حينها على المواقع الغربية المهتمة بأمن المعلومات ، وبقليل من البحث على الإنترنت عن النسخة المُسربة المسماة بـ (COFEE 1.1.2)تستطيع الحصول على نسخة منها بإذن الله ، علماً أن النسخة المُسربة قد لا تحتوي على جميع الأدوات الـتي تفوق الـ 150أداة .

ويمكنك إلقاء نظرة على موقع الأداة الرسمي على الإنترنت ، وستلاحظ الإجراءات المُعقدة للحصول على نُسخة من الأداة :

www.cofee.nw3c.org

-2-

IRCR

Incident Response Collection Report

هي عبارة عن مجموعة من الأدوات المجانية المفتوحة المصدر ، التي تقوم بجمع المعلومات من الجهاز المشتبه به ، ومُعظم هذه الأدوات موجهة لجمع المعلومات فقط دون تحليلها ، وبإمكان أي شخص أن يشغل هذه الأداة على الجهاز المشتبه به ، وبعدها يقوم بإرسال المعلومات المُستخرجة من الجهاز إلى المُحققين الرَقميين لتحليلها.

ويمكنك زيارة الصفحة الرسمية لهذه الأداة ، والحصول على نسخة منها ، على العنوان:

www.ircr.sourceforge.net

-3-

FRED

First Responder Evidence Disk

طُور برنامج FRED من قبل Jesse Kornblum لصالح مكتب التحقيقات الخاصة في القوات الجوية الأمريكية ، وذلك في خريف عام 2000، وظهر أول مرة عام 2001، والبرنامج حصري لما يسمى "فريق الاستجابة لحالات الطوارئ الحاسوبية في سلاح الجو (AFCERT) "وهي وكالة تابعة للقوات الجوية في أمريكا ، والبرنامج غير متاح للجمهور ، وهو برنامج قديم نوعاً ما ، ويوجد الكثير من الأدوات المجانية تقوم الآن بمثل عمله ، صُمم هذا البرنامج ليلتقط المعلومات سريعة الزوال "الذاكرة المؤقتة"، من جهاز المشتبه به ، وهو مشابه لبرنامج الـ IRCR، ويمكن وضع البرنامج في أصبع ذاكرة الـ USBومن ثم توصيلة بجهاز المشتبه به ، وعند تشغيله يحفظ المعلومات إلى أصبع الذاكرة ، ومن ثم يمكنك نقل أصبع الذاكرة إلى جهاز آمن لتحليله ، أو إرسال المعلومات المُستخرجة إلى المحققين الرَقميين إذا شئت .

-4-

WFT

Windows Forensisc Toolchest

تم تصميم أداة الـ WFTلتوفير آلية موثوقة وتلقائية ، عند حدوث طارئ أو حدث عَرَضي لجهاز الحاسب ، وللتدقيق أيضاً على نظام Windowsأثناء جمع المعلومات الأمنية ذات الصلة بالتحقيق من الجهاز المشتبه به ، والـ WFT تقوم أساساً على تعزيز كمية المعلومات المُستخرجة من جهاز الحاسب الآلي ، وهي ضليعة في ذلك ، كما يقول مطوروها، كما أنها تعرض المعلومات المُستخرجة من جهاز المشتبه به، على هيئة قوالب HTML، ويمكن استخدام أداة الـ WFTللبحث عن علامات وقوع اختراق في الحاسب ، أو لتأكيد سوء استخدام جهاز الحاسب ، وأُنتجت هذه الأداة لتكون مُفيدة في يد المحقق الجنائي الرَقمي في مُحاكمة المشتبه بهم ، وهي تزّود المُحقق بالكثير من المعلومات

التي يحتاجها في رفع دعوى على جميع مستخدمي جهاز الحاسب المشتبه به ، علماً أن جميع المعلومات المُستخرجة من جهاز الحاسب ، تُختبر عن طريق أكواد التشفير مثل (MD5 - SHA1)لضمان تطابق المعلومات المستخرجة من الجهاز ، مع ما يوجد في الجهاز الأصلي.
ويمكنك تحميل نسخة من الأداة من الصفحة الرسمية لها ، على هذا العنوان:

www.foolmoon.net/security/wft

-5-

FAU

Forensic Acquisition Utilities

هي مجموعة من الأدوات المُستخدمة في التحقيق الجنائي الرَقمي على أنظمة Windows، وهي مُجهزة لجمع المعلومات وتطهيرها من الشوائب ، دون المساس بالأدلة الأصلية ، وتستخدم أيضاً أكواد التشفير للتأكد من مطابقتها مع الأصل ، و من الخطأ اعتبار هذه الأداة برنامج يقوم بمنع الكتابة على الأدلة الـ (Write Blocker)، بل يستلزم وجود أجهزة منع الكتابة كطرف ثالث بين هذه الأدوات وبين الجهاز المشتبه به.
ويمكنك تحميل نسخة من الأداة من الصفحة الرسمية لها ، على هذا العنوان:

www.gmgsystemsinc.com/fau

-6-

WMFT

Windows Memory Forensics Toolkit

هي عبارة عن مجموعة من الأدوات المُخصصة لعمل المحقق الجنائي الرَقمي ، وتُستخدم لأخذ صورة الذاكرة الفعلية المكتسبة في نظام الـ Windowsمن جهاز المشتبه به وتحليلها ، ويوجد منه إصدار يعمل على نظام الـ . Linux
ويمكنك الحصول على نسخة من الـ WMFT، وغيرها من الأدوات ، على هذا العنوان:

www.rootkit.com

أخيراً...يجب أن تعلم أخي الغالي ، أن جميع البرامج التي لم نستعرضها هنا ، تقوم بنفس العمل تقريباً ، ولكن مع اختلاف بسيط في طريقة عرضها للمعلومات المُستخرجة من الجهاز المشتبه به ، إما على شكل نصي أو على هيئة واجهة رسومية ، أو تختلف في سرعة استخراج المعلومات من الجهاز المشتبه به ، أو في شمولية أداة في جلب المعلومات كاملة ، وأخرى مُختصة فقط بجلب معلومات الذاكرة المؤقتة ، أو تميز أداة عن غيرها لكونها تعمل على جميع الأنظمة ، وأخرى تستطيع من خلالها استرجاع الملفات المحذوفة والتي تم تغيير صيغها قبل الحذف ، وغير ذلك من الاختلافات البسيطة ، والله تعالى أعلم.

||||||||مواقع تقدم أدوات و دراسات حول التحقيق الجنائي الرقمي ||||||||

-1-

www.opensourceforensics.org

يُوفر هذا الموقع للمحقق الجنائي الرَقمي برمجيات مفتوحة المصدر، ليستخدمها في عمله، وتسهل له جمع المعلومات من الأجهزة، ليدلي بعدها بشهادته في المحكمة.!!
وهذا مثال لبرنامجين ، من البرامج مفتوحة المصدر والموجودة على هذا الموقع والتي تعمل على نظام Windows

-I-

TULP2G

المبرمج:

معهد الأدلة الجنائي الهولنديNetherlands Forensic Institute - NFI -

وصف الأداة:

وُضع هذا البرنامج المُتقدم ليجعل من السهل استخراج وفك شفرة البيانات من الأجهزة الرَقمية ، ويأتي برفقته إضافات مُستقلة ، تسمح بقراءة البيانات من الهواتف النقالة ، وبطاقات الـ SIM

-II-

DFF

Digital Forensics Framework

المبرمج:

Solal Jacobوآخرين

وصف الأداة:

يهدف هذا البرنامج على توفير إطار حقيقي للمُجتمع في التعامل مع أدوات التحليل الجنائي، وذلك حتى يتمكن الناس من استخدام أداة واحدة فقط في تحليل البيانات، أو كما يقول مُبرمجيه، ويوجد نسخ متعددة تعمل على أنظمة Windows & Linuxوغيرها.

ويوجد على الموقع الكثير من الأدوات التي بإمكانك أن تكتشفها بنفسك ، ويوجد شرح مُبسط لفائدة كل أداة في الموقع.

-2-

www.e-evidence.info

ويوجد فيه الكثير من المعلومات حول التحقيق الجنائي الرَقمي ، ودليل للكتب التي يُمكنك شراءها عبر الإنترنت ، والرائع في الموقع ، وجود الكثير من الدراسات والمقالات حول التحقيق الجنائي الرَقمي ، مرتبة أبجدياً ، وهي متاحة للتحميل مجاناً بصيغة الـ PDF، تجدها في قسم الـ

THE Digital Forensics Bibliography

-3-

www.digital-evidence.org

وهي مُدونة شخصية لـ Brian Carrierوهو أحد مطوري أدوات التحقيق الجنائي الرَقمي، وستجد في هذه المدونة، الأدوات التي برمجها أو شارك في تطويرها، وغيرها من المعلومات حول التحقيق الجنائي الرَقمي .

-4-

www.forensics.nl

كل شيء حول تعلم التحقيق الجنائي الرقمي كما يعرّف الموقع بنفسه ،ستجد فيه العشرات من الدراسات المجانية حول إخفاء البيانات وغيرها ، وهو موقع ضخم حقاً ، يمكنك التعرف عليه بنفسك.

و للعلم...كل موقع من هذه المواقع، تحتوي على عشرات الروابط لمواقع أخرى حول التحقيق الجنائي الرَقمي ، يُمكنك زياراتها والاستفادة منها ، ولا تنسى أيضاً أن مُحركات البحث تقوم بإيصالك إلى المزيد منها مجاناً.!!



||||||||حاجة الجهاد الإعلامي والميداني إلى خبراء في "أمن المعلومات||||||||"

إن الباحث في عالم (أمن المعلومات - Information Security) سيتضح له سعة هذا العالم الرائع ، ومدى حاجة الإعلام الجهادي ، إلى خبراء في هذا العلم المُتطور ، فخبير أمن المعلومات "الجهادي "قادر -بإذن الله -على إدارة المواقع والمُنتديات الجهادية ، وحمايتها من الاختراق ، وخبير أمن المعلومات "الجهادي "قادر-بإذن الله -على معرفة أساليب العدو في الهجوم على المواقع الجهادية ، وبالتالي سُرعة التصدي له ، وإفشال مُخططاته في مهدها ، وخبير أمن المعلومات "الجهادي "قادر-بإذن الله -على حماية معلومات أعضاء المنتديات الجهادية وتشفيرها ، وتطوير طرق التواصل الآمن بين الأعضاء والمشرفين ، ووضع أفكار جديدة في إدارة المنتديات والمواقع الجهادية ، ورفع مستوى الآمان العام للموقع الجهادي ، وإجراء الاختبارات الدورية لقياس أمان الموقع الجهادي، وقادر أيضاً على ابتكار طرق لرفع المواد الجهادية بشكل آمن ، وجعلها مُستحيلة الاكتشاف ، مما سيُفيد مراكز ومؤسسات المجاهدين الإعلامية ، وغير ذلك من الفنون الأمنية التي لا تحصى.

وما علم **(التحقيق الجنائي الرَقمي)** ، إلا واحد من عدة علوم تدخل كلها في نطاق أمن المعلومات ، وأيضاً هناك **علم التشفير**، ويدخل أيضاً تحت نطاق هذا العلم الواسع ، وكلنا **نعلم** مدى فائدة هذا العلم في حماية معلومات المجاهدين ، وفائدته في إنشاء وسائل اتصالات **مُشفرة** بين الخلايا الجهادية في الميدان ، وغير ذلك من الأفكار ، التي ستسّهل بإذن الله على المجاهدين أعمالهم وخططهم ، **فهل علمت الآن ، مدى حاجة أسود الجهاد الإعلامي والميداني ، إلى خبراء في أمن المعلومات؟!!**

||||||||المُختبر التقني "الجهادي" لأمن المعلومات ||||||||

هذه فكرة جاءتني وأنا أُعد هذه المقالة ، وتتلخص هذه الفكرة على إنشاء مُختبر تقني تحت أي مسمى بشرط أن يكون هذا المُختبر "مُعتمد من مركز الفجر "، وأن يُشرف عليه ولو **رجل واحد من خبراء أمن المعلومات المجاهدين** ، **ويكون مُزكى من القائمين على الإعلام الجهادي** ، **ومُهمة هذا المختبر التقني** ، اعتماد البرامج ، والأدوات التي يحتاجها المجاهد الإعلامي ، وذلك بعد إجراء عدة اختبارات عليها ، **وحتى تتضح الفكرة ، والهدف ، والفائدة المتوقعة من وجود مثل هذا المُختبر ، سأضرب لكم المثال التالي :**

يوجد الآن على الإنترنت العشرات من البرامج ، والأدوات التي مُهمتها إزالة أو تنظيف الذاكرة المؤقتة لجهاز الحاسب الآلي ، **السؤال هنا** أي من هذه البرامج، أو الأدوات يقوم بذلك بالفعل؟ ، وأي من هذا الأدوات نعتمده على أجهزتنا ؟

يأتي هنا دور المختبر التقني المُعتمد من القائمين على الإعلام الجهادي، وذلك بأن يقوم المختبر بثلاث خطوات كالتالي:

{ 1 }يُرشح المُختبر مجموعة من البرامج التي يُتوقع قيامها بعملية تنظيف الذاكرة المؤقته بشكل جيد ، ثم تُختبر هذه البرامج بنفس أدوات المحقق الجنائي الرَقمي ، فإذا **لم** تنجح أدوات المحقق الجنائي الرَقمي في **"استرجاع "** المعلومات من الذاكرة المؤقتة ، والتي نُظفت بواسطة البرنامج ، فيعني ذلك **نجاح** البرنامج في الاختبار.

{ 2 }يقوم المختبر التقني "الجهادي" "باعتماد النُسخة التي اجتازت الاختبار ، ثم يضع لها كود تشفير MD5في تقريره الدوري ، حتى يقوم المجاهد الإعلامي بتحميل هذا البرنامج ، و مطابقة كود التشفير للنسخة التي قام بإنزالها ، مع كود التشفير المُعلن في التقرير الدوري للمختبر ، للتأكد من أنها النسخة المُعتمدة لدى المُختبر التقني "الجهادي."

{ 3 }إصدار تقرير نصف سنوي ، أو سنوي ، يحتوي على البرامج، والأدوات المُعتمدة من المُختبر والتي اجتازت الاختبارات بنجاح ،مع أكواد التشفير الخاصة بكل برنامج تم اعتماده من المُختبر.

وأما البرامج والأدوات التي تُرشح **لدخول** المُختبر التقني "الجهادي" فهي البرامج التي تزيد من أمن المجاهد الإعلامي ، **مثل برامج الكتابة على المساحة الفارغة على القرص الـ(MFT) ، وبرامج إزالة الذاكرة المؤقتة ، وبرامج حذف الملفات بشكل يضمن عدم استرجاعها** ، وغير ذلك من البرامج التي يرى القائمين على المختبر التقني ، فائدتها في **رفع** مستوى الآمان للمجاهد الإعلامي.
ولو **لم** يصدر في التقرير الدوري السنوي أو النصف سنوي للمُختبر، سوى **3**أو **4**برامج مُعتمده لكفى ، حيث سيكون للمجاهد الإعلامي حينها مصدر آخر مُعتمد ، غير **مُبالغات** مُنتجي هذه البرامج ، والتي لا تتعدى في أكثرها ، **مجال الدعاية والإعلان**.!!

واختبار البرامج، والأدوات، وإصدار التقارير حول ذلك هو أحد أعمال المُختبر التقني الذي نستطيع وضع ركائز له مُقترحة، نرتبها كالتالي:

{ 1 }إجراء الاختبارات على البرامج والأدوات ، التي ترفع من آمان المجاهد الإعلامي ، وإصدار تقرير دوري ، يحتوي على البرامج والأدوات المعتمدة من المختبر، مع أكواد التشفير الخاصة بها ، لمطابقتها.

{ 2 }مراقبة مواقع أمن المعلومات الغربية وغيرها، وخاصة التي تهتم بتطوير أدوات المحقق الجنائي الرَقمي، وحيازة هذه الأدوات، وإتقان استخدامها، ومن ثم استخدامها في إجراء الاختبارات على البرامج والأدوات المُنتخبة.

{ 3 }إنزال شُروحات مُعتمدة لعمل البرامج والأدوات التي تم اعتمادها من المُختبر التقني "الجهادي" ، وكذلك شروحات حول طرق التصفح الآمن وغير ذلك من الأمور التقنية التي تهتم فقط في الجانب الأمني للمجاهد الإعلامي.

{ 4 }إقامة دورات في التحقيق الجنائي الرَقمي ، والتشفير، وفي أمن المعلومات بشكل عام ، وتطوير البرامج التي ابتدعها أسود الإعلام الجهادي كبرنامج "أسرار المجاهدين "وغيرها.

وللتذكير...فإن عدم قيام مثل هذه المُختبرات التقنية "الجهادية "المُعتمدة حالياً ، لا يعني بالضرورة ، التكاسل عن السعي خلف التطوير الذاتي في الجانب الأمني التقني ، وإلى أن تُقام مثل هذه المُختبرات المُعتمدة ، سنبذل جُهدنا في تطوير أنفسنا ، وإفادة بعضنا البعض بما يفتح الله به علينا ، لننصر هذا الدين بكل ما نملك، فاليوم في الإعلام الجهادي ، وغداً بإذن الله في الجهاد الميداني.

وتذكر أخي الغالي ، أن هذه مُجرد فكرة "تقنية" ، قد تكون بعزائم الصادقين، نواة لعمل إعلامي، جهادي، احترافي، ذو أمان عالي...

والله خيراً حافظاً وهو أرحم الراحمين ...

||||||||| أسود " أمن المعلومات " المجاهدين أين هم؟ !! |||||||||

بعد أن علمنا إمكانيات العدو ، وطرق عَمله ، لم يبقى لنا ، إلا أن نجتهد في معرفة أفضل السُبل لحماية حصون وأسود أمن "الإعلام الجهادي ، وخير من يُقَدم النصح في طرق التصدي للعدو ، و شن حرب مُعاكسة عليه ، هم أسود المجاهدين ، ومُحترفي حماية الشبكات والمواقع الالكترونية ، وخبراء فن " Information Security - المعلومات التشفير، وغيرهم ممن فتح الله عليهم في هذه العلوم ،
ولكن السؤال هنا .. أين هم؟ وأين نجدهم..؟

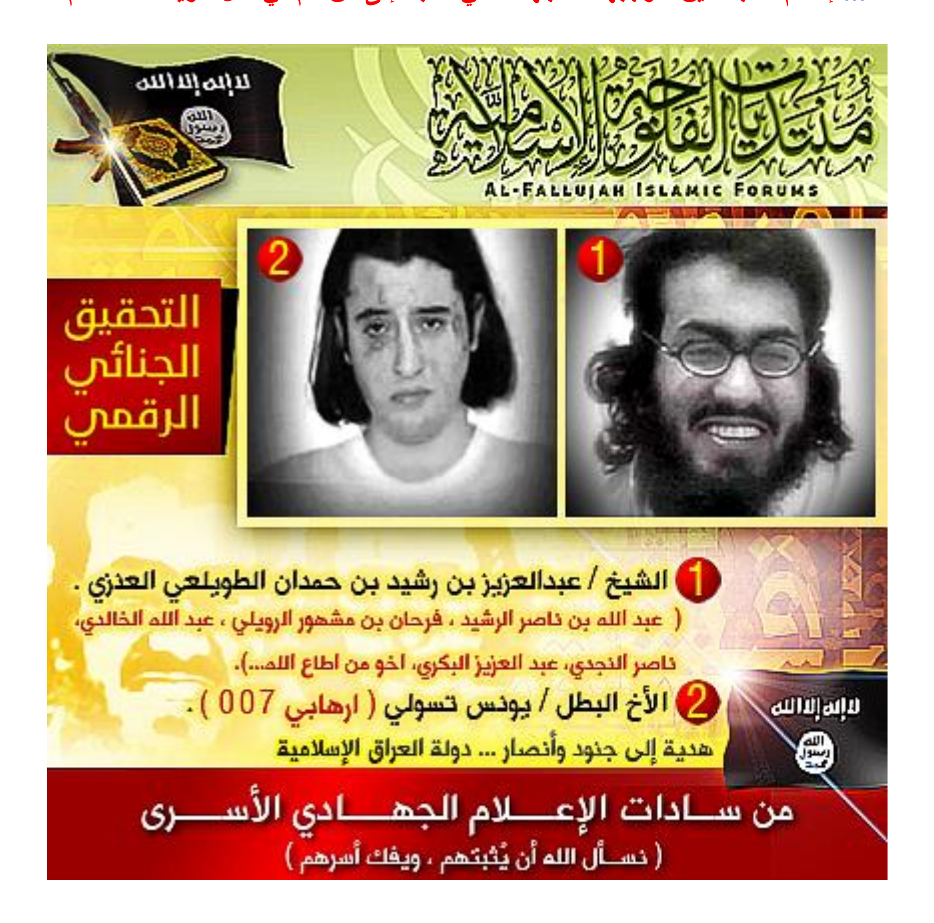
يُمكنك اقتحام .. نعم في ظرف فترة زمنية قصيرة مع نية صادقة وعزيمة حديدية !! أقول .. قد تكون أنت .. أحَدَهم !!غمار هذا العلم ، لتعود بعد فترة ، رأس حربة في هذا العلم.. فمن لها يا أسود الإعلام الجهادي؟

مع التذكير أن هذا العلم في تطور مستمر ، وكثير من الحكومات العربية وغيرها ، باتت تسعى الآن ولتوها ، لطرق باب هذا العلم ، لإطفاء شُعلة الإعلام الجهادي ، وجعل هذا العلم سلاح آخر في يدها لحربنا .

وهذا العلم ليس حكراً لحَمَلة الشهادات العُليا ، بل إن الهواة أثبتوا تفوقهم على أصحاب الشهادات الأكاديمية ، ولا نُنكر أن من المجاهدين ولله الحمد من يُتقن هذه العلوم ، وما برنامج " أسرار المجاهدين " إلا خيرُ شاهدٍ على ذلك.

لا يزال الإعلام الجهادي ، في حاجة شديدة إلى أبطال في هذا العلم ، ليرفعوا من سقف الثقافة الأمنية الرَقمية ، ...ولكن لدى عامة المجاهدين وأنصارهم.

فاستعن بالله يا بطل ، وتوكل عليه ، واصدق النية مع الله في طلب مثل هذه العلوم ، وأبشر بالخير في الدنيا والآخرة ، فإعلامُ المجاهدين ، وجبهات الجهاد ، في حاجة إلى من هم في مثل عزيمتك ، فتقدّم...



||||||||وسائل مُقترحة لِحماية "الأرشيف الجهادي" للمُجاهد الإعلامي ||||||||

هذه وسائل وأفكار مُقترحة ، أتطفل فيها على أهل الاختصاص ، وأهديها لكم يا أسود الإعلام الجهادي ، وأشهد الله أني أحبكم ، وأحبُ من يُحبكم ، ولو كنت أستطيع ، لتناقشت معكم فيها ، ولرددت على كل من يُشارك منكم ، ولكن عزائي أن جُل وقتي على الإنترنت بينكم ، ولكن تصعُب علي والله المُشاركة...

الوسائل المُقترحة كالتالي:

{ 1 }حفظ الارشيف الجهادي كاملاً في "قرص صلب خارجي " ليسهل تشفيره أولاً ، وإخفائه ثانياً ، علماً أنه يوجد الآن في الأسواق الالكترونية ، أقراص صلبة ذات سِعات مُتعددة ، وفيها خاصّية التشفير بطول 256 بت ، مثل القرص الصلب من شركة WDوالمسمى (MyPassportEssential)حيث يأتي مُدمج في القرص الصلب برنامج WDSmartWareوهو برنامج فيه الكثير من المُميزات ، ولكن الذي يُهمنا منها خاصيّة وضع كلمة سر على القرص الصلب ، وفي حالة نسيانك لكلمة السر ستفقد جميع بياناتك في الداخل فتنبه!، ويأتي في نفس القرص شرح لمميزاته بلغات عدة من بينها اللغة العربية.

{ 2 }الحرص على أن لا يوجد في داخل القرص الصلب الخارجي، أي شيء يدل على شخصيتك، كوجود اسمك، أو ملفات تدل عليك.

{ 3 }الحرص على عدم كتابة كلمة السر في مُفكرة على جهازك ، أو في ورقة بجانب جهازك ، أو غيرها ، بل في مكان واحد فقط ، في وسط رأسك.

{ 4 }إخفاء القرص الصلب الخارجي المُشفر ،الذي يحتوي على الأرشيف الجهادي ، في مكان بعيد عن مكان تواجدك الدائم.

{ 5 }عدم استخدام القرص الصلب الخارجي المُشفر ، إلا في حالة محدودة جداً كأخذ شيء منه ، أو إضافة شيء إليه ، وإرجاعه إلى مكانه الآمن.

{ 6 }اقتناء أصبعي ذاكرة USB، من أي حجم تريد، حيث يُستخدم أحَدها للاستخدامات الشخصية فقط، ولا يُستخدم أبداً في حفظ مواد جهادية ولو مؤقتاً ، وجعل الآخر كوسيلة نقل للمواد الجهادية بين جهازك الشخصي وبين القرص الخارجي المُشفر الذي يحتوي على الأرشيف الجهادي ، فمثلاً عند نزول فلم جهادي جديد ، أو مجلة جهادية أو غير ذلك من المواد الجهادية ، قم بإدخال أصبع الذاكرة "الجهادي" في جهازك ، ثم قم بتحميل الفلم الجهادي أو المجلة الجهادية وحفظها مباشرة إلى أصبع الذاكرة " الجهادي "، وبعد أن يمتلئ أصبع الذاكرة "الجهادي" بالمواد الجهادية ، يأتي الآن فقط دور القرص الصلب الخارجي المُشفر ، فتقوم بجلبه ، وتفريغ المواد الجهادية الموجودة في أصبع الذاكرة فيه ، وتُرجع القرص الصلب الخارجي المُشفر فوراً ، إلى مكانه الآمن، وذلك يعني بالطبع ، عدم حاجتك الفِعلية إلى استخدام القرص الخارجي الصلب إلا في فترات زمنية متباعدة ، حسب حجم أصبع الذاكرة لديك.

{ 7 }احرص على أن لا يوجد في جهازك الشخصي الذي تستخدمه ، أي مواد جهادية ، و لا تنسى إزالة المواقع الجهادية من مُفضلتك.

{ 8 }يجب أن تضع كلمة سر على جميع ملفاتك المهمة "جداً" وذلك بجمعها في ملف واحد ثم ضغطها باستخدام برنامج الـ WinRAR،ولأن الهدف من استخدام برنامج الضغط هو وضع كلمة سر على ملفاتنا المُهمة ، فلسنا في حاجة إذاً إلى إنقاص حجم الملفات فقم باختيار نوع الضغط Store من قائمة Compreesion method ومن مجموعة Advanced قم بوضع كلمة سر معقّدة بضغطك على Set password ومن ثم إدخال كلمة السر المعقّدة التي تحتوي على أحرف صغيرة وكبيرة ، وأرقام ، ورموز ، وأجعلها لا تقل عن 10 خانات ، وبعدها فعّل خيار الـ Encrypt file names لتشفير أسماء الملفات ، وعدم إظهارها إلا في حالة إدخالك لكلمة السر.

{ 9 }قم باستخدام البرامج التي تقوم بالكتابة على المساحة الفارغة (MFT) في القرص الصلب الخاص

بجهازك الشخصي ، كل فترة زمنية أنت تحددها ، كمرة واحدة في الشهر مثلاً ، و من البرامج المقترحة برنامج (CCleaner)حيث يُوجد فيه خاصّية الكتابة على المساحة الفارغة (MFT)حتى 35مرة ، و قد يستغرق ذلك ساعات طويلة ، حسب المساحة الفارغة في قرصك الصلب وحسب مواصفات جهازك ، حيث أن كل ما تقوم بحذفه من جهازك ، يذهب مباشرة للمساحة الفارغة (MFT)ويسهُل على الهواة استرجاع الملفات المحذوفة ، فضلاً عن الأجهزة الأمنية ، فأحرص أخي على الكتابة عليها بشكل دوري(9).

{ 10 }إذا كنت من رُواد المنتديات الجهادية ، ومن أصحاب المُشاركات فيها ، فلا تجعل في قرصك الخارجي الصلب ولا في أصبع الذاكرة "الجهادي" ما يدل على ذلك ويجب عليك حفظ)أسمك في المنتدى ، وكلمة السر ، وبريدك الإلكتروني المُستخدم في المواقع الجهادية (في رأسك فقط ، وأما مُشاركاتك التي أنزلتها في المنتدى الجهادي ، فقم بحفظها كصفحة HTMLفي ذاكرة الـ "USBالجهادية "، بعد أن تُسجل خُروج من المنتدى ، حتى تظهر المشاركة كمقالة أُعجبت بها لأحد الكتاب "المجهولين "في المنتدى الجهادي ، ومن ثم انقلها إلى ارشيفك الجهادي ، وأحرص على عدم الإحتفاظ بالملفات الأصلية لمشاركاتك الجهادية في المنتديات ، من ملفات التصاميم المفتوحة ، أو مُسودات المقالات النصية ، وغير ذلك من الأمور التي قد تكشف عن شخصيتك ، في حال الوصول إليها ، و تُستخدم كدليل ضدك ، دون الحاجة لسماع اعترافاتك !!، واجعل مكان صياغة أعمالك في أصبع الذاكرة "الجهادي" فقط ، وقم بحذفها مباشرة بعد أن تنتهي منها ، لزوال الفائدة منها ، و أما الذاكرة "الجهادية" فستقوم بإتلافها "مادياً "وشراء أخرى جديده، كل فترة زمنية أنت تحددها ، ولا تحتفظ بشيء من الملفات الأصلية لمشاركاتك على القرص الخارجي المشفر ولو مؤقتاً، اللهم إلا ما أشرت إليه من حفظها كنسخة HTML، بعد إنزالها في المنتدى الجهادي ، وبهذه الطريقة ستُخفي جميع آثار أعمالك ومشاركاتك الجهادية السابقة ، عند إتلافك لذاكرة الـ USBالجهادية.



أخيراً ...هذه مقالة تحتاج إلى تنقيح من أهل الخبرة أولاً ، ثم تحتاج إلى من يطبقها واقعاً ثانياً ، ويجب على المجاهد الإعلامي ، عدم التهاون في هذا الجانب ، بل يجب عليه فهم هذه العلوم وإتقانها ، وشرحها لمن يجهل من الإخوة...

هذا مافتح الله علي ، ويسر لي جمعه وإعداده ، أهديته لكم طمعاً في أجر نُصرتكم ، وشحذاً لهممِكم ، وأني أُشهد الله ثم أشهدكم يا عباد الله أني أحب الشيخ "الشهيد" أبو عمر البغدادي في الله ، واني والله مازلت أجمع الأموال ، وأحفظها للمجاهدين ، منذ أن دعى لذلك في أحد كلماته ، و أني أشهد الله ثم أشهدكم ياعباد الله أني أحب الشيخ "الشهيد" أبو حمزة المهاجر في الله ، وأسأل الله أن يجمعني وإياكم بهم تحت ظله يوم لا ظل إلا ظله .

اللهم أجمعني ، وأحبتي بهم في جنات النعيم ، مع النبيين ، والصديقين ، والشهداء ، والصالحين ، وحسن أولئك رفيقا.

كتبه حباً في الله لدولة العراق الإسلامية
||أبي طارق عبدالحكيم حامد ||
يوم الثلاثاء
1431/5/13هـ-2010/4/27 - م

1- هو البطل عبدالله بن حسن العسيري -رحمه الله- ، منفذ العملية الاستشهادية البطولية التي استهدفت الطُويغيت محمد نايف ، ولتتعرف أكثر على أبو الخير -رحمه الله- ، شاهد فلم أحفاد محمد بن مسلمة -رضي الله عنه - الصادر عن مؤسسة الملاحم -رمضان1430- تنظيم القاعدة في جزيرة العرب.

2- هو البطل علي بن حامد المعبدي الحربي -رحمه الله- ،أحد منفذي العملية الاستشهادية ، التي استهدفت مقر سكن الصليبيين في الرياض ، ولتتعرف أكثر على هدية المعبدي- رحمه الله- ، شاهد الفلم الرائع بدر الرياض ، مؤسسة السحاب - تنظيم القاعدة في جزيرة العرب.

3-قامت قطر ببناء قاعدة العُديد الجوية بكلفة مليار دولار في الوقت الذي لم يكن لديها أي قوة جوية. من كتاب كوبرا2 - ص78.

4- موقع وزارة داخلية قطر/ 3-1-2010.

5- الاستشهادي البطل أبو دجانة الخراساني -رحمه الله- أحد سادات الإعلام الجهادي.

6- ماذا تفعل في مسرح الجريمة الإلكترونية؟ - iSecur1ty.org

7-التحليل الجنائي الرَقمي - من سلسلة المقالات العلمية - مركز التميز لأمن المعلومات.

8- ماذا تفعل في مسرح الجريمة الإلكترونية؟ - iSecur1ty.org

9- إيرادي لبرنامج CCleaner لا يعني بالضرورة أنه أفضل الموجود ، بل هو من البرامج الشهيرة في مجاله ، و يبقى أن يُختبر من قبل " جهة موثوقة " حتى يتم اعتماده كُلياً ، وهنا تظهر فائدة ،المُختبر التقني "الجهادي" المُقترح.